Quantum Computing, Fall 2023

Dr. Fei Li
Department of Computer Science
George Mason University

Outline

1. Date: Monday
2. Time: 12:30pm-1:30pm
3. Room: EXPL 4106

Reading materials

1. `https://www.cs.umd.edu/~amchilds/qa/`
   Lecture Notes on Quantum Algorithms, by Andrew Childs (University of Maryland), 2021
2. `https://arxiv.org/abs/1907.09415`
   Quantum Computing: Lecture Notes, by Ronald de Wolf (QuSoft, CWI and University of Amsterdam), 2023
3. Some other resources

Attendance

1. Open to graduate students in Math, Computer Science, Physics, Operations Research, ECE
2. Open to faculty members and post-doctoral researchers

Weak prerequisites

1. Linear algebra
   MATH 203: Linear Algebra. 3 credits., MATH 322: Advanced Linear Algebra. 3 credits.
   MATH 321: Abstract Algebra. 3 credits., MATH 421: Abstract Algebra II. 3 credits.
2. Probability
   MATH 351: Probability. 3 credits.
3. Algorithms
   CS 483: Analysis of Algorithms. 3 credits.

Some notes

1. It is better if you have the preliminary knowledge. If not, ... We try to cover all the details.
2. We are learning these materials and the schedule is very flexible.
3. We welcome any talk to replace the topics tentatively scheduled or alternative speakers.

Tentative schedule

week	dates	materials
1	August 21	-
2	August 28	-
3	September 11	-
4	September 18	Kickoff meeting & Chapter 1 (Preliminaries)
5	September 25	Chapter 2
6	October 2	Chapter 3
7	October 9	Indigenous People's Day
8	October 16	Chapter 4
9	October 23	Chapter 5
10	October 30	Chapter 6
11	November 6	Chapter 7
12	November 13	Chapter 8
13	November 20	Chapter 9
14	November 27	Chapter 10

Outline

Notation

The Postulates of Quantum Mechanics

One qubit and its measurement

Definition (Qubit)

A qubit, $|\psi\rangle$, can be in a superposition of the 0 and 1 states.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

Any attempt to measure the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ results in $|0\rangle$ with probability $|\alpha|^2$, and $|1\rangle$ with probability $|\beta|^2$. This is known as the *Born rule* (after Max Born).

After the measurement, the system is in the measured state! That is, the post-measurement state, $|\psi'\rangle$, will be: $|\psi'\rangle = |0\rangle$ or $|\psi'\rangle = |1\rangle$. This means that we can only extract one bit of information from the state of a qubit.

The Hadamard gate: an example of interference

Definition (The Hadamard gate)

The Hadamard gate, H, has the following function on the states $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$:

$$\begin{aligned} H\,|+\rangle &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \\ H\,|-\rangle &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \end{aligned}$$

1. This is an example of “interfering” two states in superposition, to yield a deterministic outcome.
2. It is also an example of a fundamental difference between two states ($|+\rangle$ and $|-\rangle$) with the same (computational basis) measurement outcome probabilities.

The Bell state: an information theoretic way to represent entanglement

The (two-qubit) Bell state $|\Phi^+\rangle$ is defined:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

What this says is:

1. Each of the two qubits are in an equal superposition of the $|0\rangle$ and $|1\rangle$ states.
2. However, they are entangled, as soon as one qubit is measured (say the outcome is 1) then the second qubit collapses into the state $|1\rangle$.
3. There is no requirement that the two qubits are local, in the spatial sense, in order for this to occur.

Tensor multiplication

A form of multiplication on matrices: tensor multiplication. Let A and B be matrices of any dimension:

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & & \\ a_{n1}B & \cdots & a_{nm}B \end{bmatrix}$$

$$(A \otimes B)(x \otimes y) = (Ax) \otimes (By)$$

Dirac notation

When tensor multiplying vectors expressed as kets, the following are all equivalent: $|\psi\rangle \otimes |\phi\rangle$, $|\psi\rangle\, |\phi\rangle$, $|\psi\phi\rangle$.
In general, the computational basis for C^n is

$$|1\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, |2\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, |n\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

In general, if we have the composition of n two-level systems, then the computational basis is such that:

1. When expressed as a ket, the number inside the ket is a n-bit binary number. Let this number be i.
2. When expanded as a vector, we get a 2^n element vector, where each element is equal to zero, except for a single element equal to one, at the ith element (where the elements are indexed from 0 to $2^n - 1$).

Expanding vectors and matrices in the standard basis

Any vector $|u\rangle = [a_1 a_2 \ldots a_n]^T$ can be expressed as a weighted sum of standard basis vectors:

$$|u\rangle = a_1 |1\rangle + a_2 |2\rangle + \cdots + a_n |n\rangle$$

Similarly, any matrix can be expressed as a double sum over the outer-products of standard basis vectors:

$$\begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ldots & \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} |i\rangle \langle j|$$

Eigenvectors and eigenvalues

If a $n \times n$ matrix, A, has the effect of scaling a given (non-zero) vector, $|v\rangle$ by a constant, λ, then that vector is known as an eigenvector, with corresponding eigenvalue λ:

$$A\,|v\rangle = \lambda\,|v\rangle$$

The eigenvalues of a matrix are the roots of the characteristic polynomial:

$$\det(A - \lambda I) = 0$$

where det denotes the determinant, and I is the $n \times n$ identity. Each square matrix has at least one eigenvalue.

1. The determinant of a matrix is the product of its eigenvalues.
2. The trace of a square matrix is the sum of its leading diagonal elements. It is also the sum of its eigenvalues.

Normal, Hermitian and unitary matrices

1. A matrix is normal if $A^\dagger A = AA^\dagger$. If $A = A^\dagger$ a matrix is Hermitian.
2. A matrix is unitary if $A^\dagger A = AA^\dagger = I$ (the identity).

Theorem

A matrix is normal if and only if it is diagonalizable. All eigenvalues of unitary matrices have absolute value one.

Proof.

To be filled later, with an example in KLM07. □

Outline

Notation

The Postulates of Quantum Mechanics

The four postulates of quantum mechanics

Quantum mechanics is not a physical theory, but rather a framework for the development of physical theories.

1. State space: how to describe a quantum state.
2. Evolution: how a quantum state is allowed to change with time.
3. Measurement: the effect on a quantum state of interaction with a classical system that yields classical information.
4. Composition: How to compose multiple quantum systems.

State space

Postulate

Associated to any isolated physical system is a complex vector space with an inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.

Examples of physical realizations of qubits (quantum states with space C^2):

1. The spin of an electron.
2. The polarisation of a photon.
3. The current in a superconducting circuit.

Evolution

Postulate

The time evolution of the state of a closed quantum system is described by the Schrodinger equation:

$$i\hbar \frac{d \left|\psi\right\rangle}{dt} = H \left|\psi\right\rangle$$

where $\hbar$ is the physical constant, Planck's constant and H is a fixed Hermitian operator known as the Hamiltonian of the closed system.

Proof.

To be filled later. □

The change in the state of a closed quantum system from t_0 to t_1 is described by the unitary transformation:

$$\left|\psi_{t1}\right\rangle = U \left|\psi_{t_0}\right\rangle$$

Evolution

The Schrodinger equation:

$$i\hbar\frac{d\left|\psi\right\rangle}{dt} = H\left|\psi\right\rangle$$

has a solution

$$\begin{aligned}\left|\psi_{t1}\right\rangle &= e^{\frac{-iH(t_1-t_0)}{\hbar}}\left|\psi_{t0}\right\rangle \\ &= \exp\left(\frac{-iH(t_1-t_0)}{\hbar}\right)\left|\psi_{t0}\right\rangle \\ U(t_0,t_1) &= \exp\left(\frac{-iH(t_1-t_0)}{\hbar}\right)\end{aligned}$$

$U^\dagger U = \exp\left(\frac{-iH(t_1-t_0)}{\hbar}\right)\exp\left(\frac{iH(t_1-t_0)}{\hbar}\right) = e^0 = I$, where 0 denotes a zero-matrix.

The Paudi matrices

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = i \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\begin{aligned} X\left|0\right\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \left|1\right\rangle \\ Y\left|0\right\rangle &= i \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = i \begin{bmatrix} 0 \\ 1 \end{bmatrix} = i\left|1\right\rangle \\ Z\left|0\right\rangle &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \left|0\right\rangle \end{aligned}$$

$$X\left|1\right\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \left|0\right\rangle \quad Y\left|1\right\rangle = -i \begin{bmatrix} 1 \\ 0 \end{bmatrix} = -i\left|0\right\rangle \quad Z\left|1\right\rangle = - \begin{bmatrix} 0 \\ 1 \end{bmatrix} = -\left|1\right\rangle$$

The Hadamard matrix

Hadamard matrix:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Which has the following effect on the computational basis states:

$$\begin{aligned} H\left|0\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right) = \left|+\right\rangle \\ H\left|0\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right) = \left|-\right\rangle \end{aligned}$$

It puts the computational basis states in superposition. H is self-inverse, therefore:

$$H\left|+\right\rangle = \left|0\right\rangle, H\left|-\right\rangle = \left|1\right\rangle$$

i.e., it interferes the superposition to recover the original computational basis states.

Measurement

Postulate

Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment.
If the state of the quantum system is $|\psi\rangle$ directly before the measurement, the probability of the mth outcome is given by:

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$$

and the state of the system after the measurement is

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}$$

It is necessary that the probabilities of all possible outcomes sum to one, that is

$$\sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = 1$$

as $|\psi\rangle$ is arbitrary and not dependent on the index m, we can see that this is satisfied by the completeness equation,

$$\sum_m M_m^\dagger M_m = I$$

$$\begin{aligned} \sum_m p(m) &= \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = \langle\psi| \left(\sum_m M_m^\dagger M_m\right) |\psi\rangle \\ &= \langle\psi| I |\psi\rangle = \langle\psi|\psi\rangle = 1 \end{aligned}$$

This proves that the completeness equation is sufficient, and we can readily see that $\sum_m M_m^\dagger M_m = I$ is the only condition that achieves this for general $|\psi\rangle$, so therefore it is necessary too.

Measurement in the computational basis

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \qquad M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

which we can verify satisfies the completeness equation:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}^\dagger \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}^\dagger \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Note that the measurement operators, M_0 and M_1 are projectors onto $|0\rangle$ and $|1\rangle$, respectively, and for this reason it is known as a projective measurement.

Now let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ we have that

$$p(M_0) = |\alpha|^2 \qquad p(M_1) = |\beta|^2$$

Global and relative phase

We can write any one-qubit state as:

$$|\psi\rangle = e^{i\theta}(\alpha|0\rangle + \beta e^{i\phi}|1\rangle) = e^{i\theta}|\psi'\rangle$$

where α and β are positive real numbers. θ is known as the global phase, and has no observable consequences because:

$$\begin{aligned} U|\psi\rangle &= Ue^{i\theta}(\alpha|0\rangle + \beta e^{i\phi|1\rangle}) \\ &= e^{i\theta}U(\alpha|0\rangle + \beta e^{i\phi}|1\rangle) = e^{i\theta}U|\psi'\rangle \end{aligned}$$

and for any measurement operator P_m,

$$\langle\psi| P_m^\dagger P_m |\psi\rangle = \langle\psi'| e^{i\theta} P_m^\dagger P_m e^{i\theta} |\psi'\rangle = \langle\psi'| e^{i\theta} P_m^\dagger P_m |\psi'\rangle$$

where we use the fact that $(e^{i\theta}|\psi'\rangle)^\dagger = \langle\psi'| e^{-i\theta}$.
Thus we typically neglect global phase. The same cannot, however be said for the relative phase, ϕ.

Any one-qubit state is:

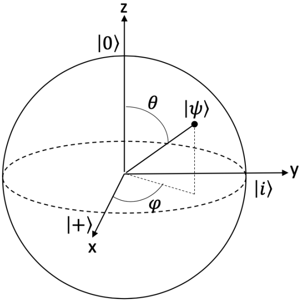
$$|\psi\rangle = e^{i\theta}(\alpha|0\rangle + \beta e^{i\phi}|1\rangle)$$

where α and β are positive real numbers. θ is known as the global phase. Ignore the global phase, we have

$$|\psi\rangle = \alpha|0\rangle + \beta e^{i\phi}|1\rangle$$

Setting $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = \sin\left(\frac{\theta}{2}\right)$ with $|\alpha|^2 + |\beta|^2 = 1$, we have

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

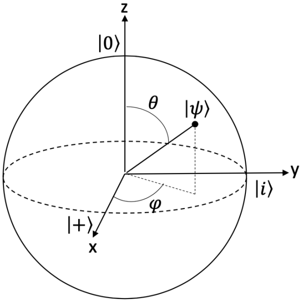


Consider a qubit $\alpha |0\rangle + \beta |1\rangle$ where α and β are complex numbers. Define (a, b) as (a', b') to be *equivalent* if there is a unit complex number c such that $a' = ca$ and $b' = cb$. Then $|a'|^2 = |a|^2$ and $|b'|^2 = |b|^2$, so the probability are the same, but the difference in complex phase is the same between a' and b' as between a and b. So if we take (a, b) as representing this equivalence class, we may as well assume that the phase of a is zero, which means that a is a non-negative real number. Let ϕ be the phase angle of b. This leaves the two real numbers b_1, b_2 used to write $b = b_1 + b_2 i$.

They are constrained by the requirement that $1 = |a|^2 + |b|^2 = a^2 + b_1^2 + b_2^2$. So we can represent the entire quantum state by the following

1. A real number between 0 and 1, without loss of generality of the form $a = \cos\left(\frac{\theta}{2}\right)$, where $0 \leq \theta \leq \pi$.
2. The phase angle ϕ, which makes $b = e^{i\phi} sin\left(\frac{\theta}{2}\right)$.

The angel θ is a latitude, and the angle ϕ is a longitude.

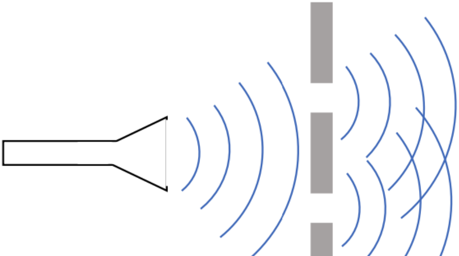


Orthogonal states are co-polar points on the Bloch sphere surface. The Pauli X, Y and Z operations are rotations of π radians around the x, y and z axes respectively.

From double-slits to qubits

1. The double-slit experiment was one of the first demonstrations of quantum phenomena. It also provides a nice visualisation of why relative phase matters but global phase does not, and gives some insight into exactly what it means "to measure a quantum system."
2. The electric field can be used to describe the effect of a propagating electromagnetic wave at a given point in space, so we now consider the electric field at the transmitting source, which in general can be expressed (in a simplified manner) as:

$$E = E_0 e^{i\omega t}$$



$$E = E_0 e^{i\omega t}$$

where E is the electric field, E_0 is a constant, ω is the angular frequency ($\omega = 2\pi f$ where f is the frequency) and t is time.
This oscillating electric field then propagates at the speed of light, so if the distance to each of the slits is d, then if we denote the locations of the upper and lower slits "u" and "l" respectively, we get that the electric field at the slits is:

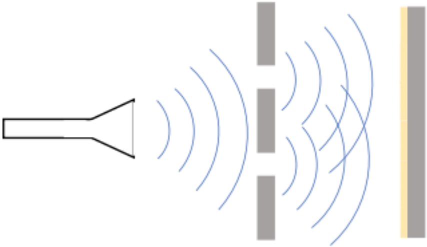
$$E(u) = E_u e^{i\left(\omega\left(t-\frac{d}{c}\right)\right)} = E_u e^{i\omega t} e^{-i\omega\frac{d}{c}}$$

for some constant E_u, and where c is the speed of light.
Thus the d/c term simply represents the time lag incurred by the wave travelling to the slit. We can also express the electric field at the lower slit

$$E(l) = E_l e^{i\omega t} e^{-i\omega\frac{d}{c}}$$

for some constant E_l.

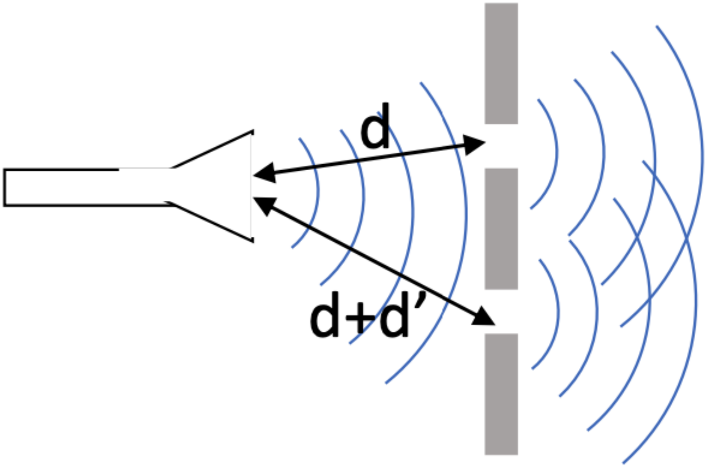
The electric field to the right-hand side corresponds to the superposition (sum) of electric fields $E(u)$ and $E(l)$ emanating from the upper- and lower-slits respectively. That is, the wave propagates as if there were two light sources, one at either slit. This means that waves from the two light sources will interfere. We will observe an interference pattern, corresponding to the constructive and destructive interference:



It follows that the mathematical description of a quantum system should be sufficient to allow both possibilities – it should both enable the (probabilistic) measurement outcomes to be determined, and also fully capture the subsequent wave propagation (if a measurement is not made). In particular, according to Postulate 1 of quantum mechanics, the system is completely described by its state vector, thus the quantum state at the double slit must completely capture everything about the wave-particle duality.

For a two-level quantum system (qubit), we can qualitatively appreciate that a complex superposition over computational basis vectors has the required ingredients. The computational basis vectors ($|0\rangle$ and $|1\rangle$) represent the binary states which can occur if measured (i.e., which slit the photon has passed through) – and the complex coefficients thereof allow the probabilities of each to be evaluated, but also are sufficient to allow the subsequent wave-propagation (i.e., to the right-hand side of the screen) to be expressed if a measurement is not made (and this is why they must be complex).

The double-slit experiment also provides us with a sketch of why relative phase is important, but global phase is not.



If we adjust the double slit so that the lower of the slits is now a distance $d + d'$ from the source, as shown above, we get electric fields at the upper slit

$$E(u) = E_u e^{i\omega t} e^{-i\omega \frac{d}{c}}$$

as before, but for the lower slit

$$E(l) = E_l e^{i\omega t} e^{-i\omega \frac{d+d'}{c}} = E_l e^{i\omega t} e^{-i\omega \frac{d}{e}} e^{-i\omega \frac{d'}{e}} = E_l e^{i\omega t} e^{-i\omega \frac{d}{c}} e^{-i\phi}$$

where we define $\phi = \omega \frac{d'}{c}$.

If we now want to know the electric field at some point "p" equidistant from the two slits (and to the right-hand side of by a distance d''), we simply add the electric fields

$$\begin{aligned} E(p) &= E'_u e^{i\omega t} e^{-i\omega\frac{d}{c}} e^{-i\omega\frac{d''}{c}} + E'_l e^{i\omega t} e^{-i\omega\frac{d}{c}} e^{-i\phi} e^{-i\omega\frac{d''}{c}} \\ &= e^{-i\omega\frac{d}{c}} e^{-i\omega\frac{d''}{c}} e^{i\omega t} (E'_u + E'_l e^{-i\phi}) \end{aligned}$$

where the constants E'_u and E'_l have been defined to allow for further reduction in electric field magnitude owing to the further propagation. If we let $E'_u \approx E'_l$ then we can express this as:

$$E(p) = E'_u e^{-i\omega\frac{d+d''}{c}} e^{i\omega t} (1 + e^{-i\phi}$$

We can see that $E'_u e^{-i\omega\frac{d+d''}{c}}$ is a constant that has been "factored out", and the constant $-\omega\frac{d+d''}{c}$ is the global phase, which has only a classical effect.
However, the quantum element of the wave's behaviour only concerns how the two superposed components interfere (and thus the probabilities of measurement outcomes at various points in the evolution), and this is determined only by the relative phase $-\phi$.

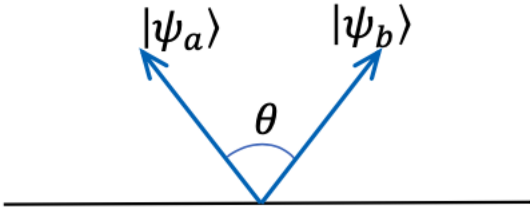
Helstrom-Holevo bound

Theorem

If $|\psi\rangle$ is either $|\psi_a\rangle$ or $|\psi_b\rangle$, where $\langle\psi_a|\psi\rangle_b = \cos\theta$, then the probability of correctly inferring the state $|\psi\rangle$ is less than or equal to $\frac{1+\sin\theta}{2}$.

Proof.

To be filled in later. □



Composition

Postulate

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

1. Single qubit unitary matrices applied to a separable state leads to a separable state.
2. CNOT is an entangling operation.

Some “no-go” theorems

1. To get a physical grasp of the quantum world.
2. Often used in theoretical work, e.g., a constructive proof is used to show that something is achievable, and the converse is related to a known “no-go” theorem.

The no-signalling principle: set-up

Alice and Bob are at different ends of the universe, but each have one half of a Bell pair: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

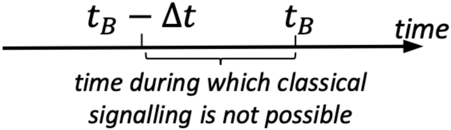
1. Alice can measure her qubit whenever she wants, and this will collapse Bob's to the same state.
2. We are interested in whether Bob can infer whether or not Alice has measured her qubit.
3. But all that Bob can do to infer whether Alice has measured her qubit is to measure his own qubit – therefore, the question reduces to whether the measurement probabilities that Bob sees are altered by virtue of Alice having performed her measurement.

If Bob can infer from measurement of his qubit whether or not Alice has measured hers, then this does enable faster than the speed-of-light information transfer. Consider the following set-up.

1. Alice and Bob are spatially separated by a distance that takes light Δt seconds to traverse.
2. Bob is interested in whether some event that Alice witnesses has occurred before time t_B.

When Alice witnesses the event she will signal to notify Bob. So we have two alternatives:

1. If Alice uses classical signalling, then if the event occurs less than Δt seconds before t_B, then there is no way she can send a signal to Bob that he will receive before t_B.
2. However, if Alice can send a signal solely by measuring her qubit, then she can signal instantly, and hence notify Bob of the event any time up to t_B.



The no-signalling principle also holds for any type of entanglement, and also any scheme Alice and Bob may come up with involving transformations of their qubits, and measurements in arbitrary bases.

The no-cloning principle

Theorem

Therre is a quantum state $|\psi\rangle$ and a register initially set to $|0\rangle$, and there is no such a cloning unitary, U such that:

$$U(|\psi\rangle\,|0\rangle) = |\psi\rangle\,|\psi\rangle$$

Proof.

Consider that U must clone all quantum states, so as well as $U(|\psi\rangle\,|0\rangle) = |\psi\rangle\,|\psi\rangle$. We have that $U(|\phi\rangle\,|0\rangle) = |\phi\rangle\,|\phi\rangle$
Taking the inner products of the left- and right-hand sides of the above equations, we have that:

$$\begin{aligned}
\langle\psi|\,\langle 0|\,U^{\dagger}U\,|\phi\rangle\,|0\rangle &= \langle\psi|\,\langle\psi|\phi\rangle\,|\phi\rangle \\
\langle\psi|\phi\rangle\,\langle 0|0\rangle &= (\langle\psi|\phi\rangle)^2 \\
\langle\psi|\phi\rangle &= (\langle\psi|\phi\rangle)^2
\end{aligned}$$

which is only true if $\psi = \phi$ or ψ and ϕ are orthogonal.